

Examples of subgroups

Def 1

Center of a group

The center of a group G is the subset of elements in G that commute with every element in G .

Notation : $Z(G)$

$Z \rightarrow$ German word
Zentrum
(center)

$$Z(G) = \{ a \in G \mid ax = xa \ \forall x \in G \}$$

Thm

Center of a group G is a subgroup of G

Proof:

$$\therefore e \in G$$

$$x = ex = xe \ \forall x \in G$$

$$\therefore e \in Z(G)$$

$\therefore Z(G)$ is a nonempty set.

1-

$$(1) \ a, b \in Z(G) \Rightarrow ab \in Z(G)$$

$$(2) \ a \in Z(G) \Rightarrow a^{-1} \in Z(G)$$

$$\text{Let } a, b \in Z(G)$$

$$ax = xa \quad \forall x \in G,$$

$$bx = xb \quad \forall x \in G$$

$$(ab)x = a(bx) \quad \left\{ \begin{array}{l} \text{Associativity} \end{array} \right\}$$

$$= a(xb) \quad (\because bx = xb)$$

$$= (ax)b \quad (\text{Associativity})$$

$$= (xa)b \quad (\because ax = xa)$$

$$= x(ab) \quad (\text{Associativity})$$

$$\therefore ab \in Z(G).$$

Now, we need to show $a \in Z(G) \Rightarrow a^{-1} \in Z(G)$

$$\text{i.e.} \quad a^{-1}x = xa^{-1} \quad \forall x \in G$$

$$\text{Let } a \in Z(G) \Rightarrow ax = xa$$

$$ax = xa$$

$$a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$$

$$(a^{-1}a)(xa^{-1}) = (a^{-1}x)(aa^{-1})$$

$$e(xa^{-1}) = (a^{-1}x)e$$

$$xa^{-1} = a^{-1}x.$$

$$\Rightarrow a^{-1}(ax) = a^{-1}xa$$

$$\Rightarrow (a^{-1}a)x = a^{-1}xa$$

$$\Rightarrow ex = a^{-1}xa$$

$$\Rightarrow x = a^{-1}xa$$

$$\Rightarrow xa^{-1} = a^{-1}xa a^{-1}$$

$$\Rightarrow xa^{-1} = (a^{-1}x)(aa^{-1})$$

$$\Rightarrow xa^{-1} = (a^{-1}x)e$$

$$\Rightarrow xa^{-1} = a^{-1}x$$

$$\Rightarrow a^{-1}x = xa^{-1}$$

$$\Rightarrow a^{-1} \in Z(G)$$

By Two step subgroup test, $Z(G)$ is a Subgroup of G .

Def ②

Centralizer of an element

Let a be a fixed element of a group G .

Then the Centralizer of a in G is the set of all elements in G that commutes with a .

Notation: $C(a)$

$$C(a) = \{ g \in G \mid ga = ag \}$$

Thm

show that Centralizer of an element is a subgroup of a group

Proof:

Let G be a group and a be a fixed element of G .

$$\therefore ae = ea$$

$$\Rightarrow e \in C(a)$$

Now let $g_1, g_2 \in C(a)$

$$\therefore g_1 a = a g_1 \text{ and } g_2 a = a g_2$$

$$\begin{aligned}
 \text{Now } (g_1 g_2) a &= g_1 (g_2 a) = g_1 (a g_2) \\
 &= (g_1 a) g_2 = (a g_1) g_2 \\
 &= a (g_1 g_2)
 \end{aligned}$$

$$\therefore g_1 g_2 \in C(a)$$

Now let $g \in C(a)$

$$\Rightarrow ga = ag$$

$$\Rightarrow \bar{g}^{-1} (ga) \bar{g}^{-1} = \bar{g}^{-1} (ag) \bar{g}^{-1}$$

$$\Rightarrow (\bar{g}^{-1} g) (a \bar{g}^{-1}) = (\bar{g}^{-1} a) (g \bar{g}^{-1})$$

$$\Rightarrow e(a \bar{g}^{-1}) = (\bar{g}^{-1} a) e$$

$$\Rightarrow a \bar{g}^{-1} = \bar{g}^{-1} a$$

$$\Rightarrow \bar{g}^{-1} a = a \bar{g}^{-1}$$

$$\Rightarrow \bar{g}^{-1} \in C(a)$$

By two step subgroup test,

$C(a)$ is a subgroup.

Example: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, $+_4$

$$Z(G) = \{0, 1, 2, 3\} = \mathbb{Z}_4$$

$$Z(G) = \{g \in G \mid ax = xa \ \forall x \in G\}$$

$$C(1) = \{0, 1, 2, 3\} \quad C(a) = \{g \in G \mid ga = ag\}$$

$$= \mathbb{Z}_4$$

$\mathbb{Z}_4$ is an abelian group ($ab = ba \ \forall a, b \in \mathbb{Z}_4$)

Note:

If G is an abelian group.

Then (i) $Z(G) = G$

(ii) $C(a) = G$ for any fixed element $a \in G$.

Example:

Operation $\rightarrow$ Multiplication

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \rightarrow$ Quaternion group

$$i^2 = j^2 = k^2 = -1$$

$$ij = k, \quad jk = i, \quad ki = j$$

$$ji = -k, \quad ki = -i, \quad ik = -j$$

H.W. Show that Q_8 is a group.

$G = Q_8$

$$Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}$$

$$Z(G) = \{1, -1\}, \quad C(1) = G = Q_8$$

$$C(i) = \{1, -1\}$$

$$C(-1) = \{\pm 1, \pm i, \pm j, \pm k\} = Q_8$$

$$C(j) = \{1, -1\}$$

$$C(k) = \{1, -1\}$$

Note: If e is the identity element of group G .
then $C(e) = G$.

Q. Show that $H = \{1, -1\}$ is a subgroup of $\mathbb{Q}_8$.

sm

$$(1)(-1) = -1, (1)(1) = 1, (-1)(1) = -1 \in H \\ (-1)(-1) = 1 \in H$$

By finite subgroup test,
 H is a subgroup of $\mathbb{Q}_8$.

Cyclic Group:

A group G is called cyclic if there is an element a in G such that

$$G = \{a^n \mid a \in \mathbb{Z}\}$$

This element a is called the generator of the group G .

Notation: $G = \langle a \rangle$

Example:

① $\mathbb{Z}_4$ is a cyclic group.

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

generator $\rightarrow 1$

generator $\rightarrow 3$

2 can't be

$$1^1 = 1$$

$$1^2 = 1 + 1 = 2$$

$$1^3 = 1 + 1 + 1 = ?$$

generator $\rightarrow 3$

2 cannot be the generator

2 cannot generate 1 and 3.

$$3^1 = 3, \quad 3^2 = 2$$

$$3^3 = 1, \quad 3^4 = 3 + 3 + 3 + 3 = 0$$

$$1^3 = 1 + 1 + 1 = 3$$

$$1^4 = 1 + 1 + 1 + 1 = 4 \pmod{5} = 4$$

② $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

5

generator $\rightarrow 2, 3$

$$3^1 = 3$$

$$3^2 = 3 \cdot 3 = 9 \pmod{5} = 4$$

$$3^3 = 2$$

$$3^4 = 1$$

$$4^1 = 4$$

$$4^2 = 16 \pmod{5} = 1$$

$$4^3 = 4, \quad 4^4 = 1$$

4 cannot generate

2 and 3

$\therefore 4$ cannot be the generator.

$$\begin{cases} 2^1 = 2 \\ 2^2 = 4 \\ 2^3 = 3 \\ 2^4 = 1 \end{cases}$$

Example:

$(\mathbb{Z}, +)$ is a cyclic group.

generator $\rightarrow 1$

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

$$1^2 = 1 + 1 = 2, \quad 1^3 = 1 + 1 + 1 = 3,$$

$$1^4 = 1 + 1 + 1 + 1 = 4$$

$$1^0 = e = 0.$$

$$(1)^{-1} = -1,$$

$$\begin{aligned} (1)^{-2} &= \{(1)^{-1}\}^2 = (-1)^2 \\ &= (-1) + (-1) = -2 \end{aligned}$$

$$a \in G, \quad b \in a^{-1} = -1a.$$

$$(1)^{-3} = \{(1)^{-1}\}^3 = 1 - 1 - 1 = -3$$

$$a \in G, \quad b \in a^{-1}$$

$$ab = e = ba$$

$$a+b = e = b+a$$

$$1+2 = 0$$

1 is the

generator of $\mathbb{Z}$.

-1 is the

generator of $\mathbb{Z}$

$$(1)^{-3} = \{(1)^{-1}\}^3 = (-1)^3$$

$$= (-1) + (-1) + (-1) = -3.$$